
Security Controls for Data Protection over the Virtual Data Center (Plano, TX)

FINAL AUDIT REPORT



ED-OIG/A11J0006
September 2010

Our mission is to promote the efficiency, effectiveness, and integrity of the Department's programs and operations.



U.S Department of Education
Office of Inspector General
Information Technology
Audit Division
Washington, DC

NOTICE

Statements that managerial practices need improvements, as well as other conclusions and recommendations in this report represent the opinions of the Office of Inspector General. Determinations of corrective action to be taken will be made by the appropriate Department of Education officials.

In accordance with Freedom of Information Act (5 U.S.C. § 552), reports issued by the Office of Inspector General are available to members of the press and general public to the extent information contained therein is not subject to exemptions in the Act.



UNITED STATES DEPARTMENT OF EDUCATION
OFFICE OF INSPECTOR GENERAL

Information Technology
Audit Division

September 29, 2010

Memorandum

TO: William J. Taggart
Chief Operating Officer
Federal Student Aid

FROM: Charles E. Coe /s/
Assistant Inspector General
Information Technology Audits and Computer Crime Investigations
Office of Inspector General

SUBJECT: Final Audit Report
Security Controls for Data Protection over the Virtual Data Center (Plano, TX)
Control Number ED-OIG/A11J0006

Attached is the subject final audit report that covers the results of our review of Security Controls for Data Protection over the Virtual Data Center for the period June 2008 through August 2010. An electronic copy has been provided to your Audit Liaison Officer(s). We received your comments concurring, partially concurring, or non-concurring with the findings and recommendations in our draft report.

Corrective actions proposed (resolution phase) and implemented (closure phase) by your office(s) will be monitored and tracked through the Department's Audit Accountability and Resolution Tracking System (AARTS). ED policy requires that you develop a final corrective action plan (CAP) for our review in the automated system within 30 days of the issuance of this report. The CAP should set forth the specific action items, and targeted completion dates, necessary to implement final corrective actions on the findings and recommendations contained in this final audit report.

In accordance with the Inspector General Act of 1978, as amended, the Office of Inspector General is required to report to Congress twice a year on the audits that remain unresolved after six months from the date of issuance.

In accordance with the Freedom of Information Act (5 U.S.C. §552), reports issued by the Office of Inspector General are available to members of the press and general public to the extent information contained therein is not subject to exemptions in the Act.

We appreciate the cooperation given us during this review. If you have any questions, please call Therese Campbell at 202-245-7367.

Enclosure

cc: Danny Harris, Chief Information Officer, (CIO)
Richard Gordon, CIO, Federal Student Aid (FSA)
Phill Loranger, Acting Director for Information Assurance and Computer Information
Security Officer, Office of Chief Information Officer
Marge White, Audit Liaison for FSA
Bucky Methfessel, Senior Counsel for Information & Technology, Office of General
Counsel (OGC)
Randy Prindle, Post Audit Group, OCFO
L'Wanda Rosemond, AARTS Administrator, OIG

EXECUTIVE SUMMARY

The U.S. Department of Education (Department), through Federal Student Aid (FSA), administers programs that are designed to provide financial assistance to students enrolled in postsecondary education institutions as well as collect outstanding student loans. FSA has consolidated many of its student financial aid program systems into a common operating environment called the Virtual Data Center (VDC) to improve interoperability and reduce costs. The VDC is considered by the Department to be a general support system and consists of networks, mainframe computers, operating system platforms, and the corresponding operating systems. The VDC is managed by Perot Systems Government Services, Inc. (contractor) and is located at the contractor facility in Plano, TX. The VDC serves as the host facility for FSA systems that process student financial aid applications (grants, loans, and work-study), provide schools and lenders with eligibility determinations, and support payments from and repayment to lenders. FSA systems hosted in the VDC include the Financial Management System, Central Processing System, Debt Management and Collection System, National Student Loan Data System, Post-Secondary Education Participants System, and Direct Loan Consolidation System, among others. Fiscal Year (FY) 2009 costs for the VDC were over \$63 million and FY 2010 budgeted costs were over \$59 million.

The Privacy Act and Freedom of Information Act mandate that the Department and FSA safeguard and protect its privacy information against unauthorized use. The Privacy Act pertains to records that have social security numbers, personal addresses, salary, and credit history stored within them. The VDC contains private financial data of students and their parents; these data are covered by the Privacy Act and its unauthorized release may be detrimental to the students or their families. It also contains propriety information of lenders, contractors, and vendors. The unauthorized release of this information would put lenders, contractors, and vendors at competitive disadvantage. While the disclosure of a single financial record can affect a student or his family, the availability and integrity of the Federal Student Aid system is of crucial importance to the nation. Billions of dollars of financial aid funds have to be allocated in a timely and accurate manner.

The objective of our audit was to perform an independent review to determine whether the Department and FSA have effective IT security controls for data protection over the VDC in accordance with the E-Government Act (Public Law 107-347), including Title III, the Federal Information Security Management Act of 2002. Our audit covered the period from June 2008 through August 2010.

FSA had adequate operational controls in place for the VDC over maintenance and personnel security. They also had adequate safeguards in place over physical and environmental controls. However, FSA did not have adequate operational controls in place over configuration management, system and information integrity, contingency planning, media protection, and awareness and training. In addition, FSA needs to improve all four technical controls of access

controls, systems and communications protection, identification and authentication, and audit and accountability.

Operational and Technical Controls Findings

Finding No. 1 - FSA needs to improve the VDC configuration management program. Specifically, FSA did not ensure that the contractor:

- Securely configured three devices connected to the network;
- Properly protected personally identifiable information (PII) (Modified Repeat Condition);
- Performed patch management adequately and timely (Modified Repeat Condition); and
- Adequately managed configuration settings and least functionality.

Finding No. 2 - FSA did not ensure that the contractor adequately identified, reported, and corrected information system flaws.

Finding No. 3 - FSA needs to improve access controls. Specifically, FSA did not:

- Perform all quarterly reviews of system accounts;
- Accurately manage inactive accounts on 3 of 12 devices or systems reviewed;
- Adequately enforce least privilege and separation of duties on the VDC users with administrator-level accounts in Active Directory and three mainframes (Modified Repeat Condition); and
- Ensure the contractor adequately enforced login access, system use, and remote access on VDC devices.

Finding No. 4 - FSA did not adequately manage system and communication protection controls. Specifically, FSA did not ensure the contractor adequately configured routers, switches, and firewalls to protect Department data and resources. In addition, FSA's policies included conflicting guidance.

Finding No. 5 - FSA did not ensure the contractor adequately configured servers, routers, switches, and firewalls for identification and authentication controls (Modified Repeat Condition).

Finding No. 6 - FSA did not adequately manage auditable events.

Finding No. 7 - FSA needs to improve contingency planning. Specifically, FSA did not:

- Ensure that the contractor encrypted and maintained backup media for three mainframe systems at offsite storage (Repeat Condition); and
- Adequately manage contingency planning for telecommunications services.

Finding No. 8 - FSA did not ensure that the contractor adequately labeled backup media containing PII sent to the VDC offsite storage (Modified Repeat Condition).

Finding No. 9 - FSA did not ensure that 3 of 74 VDC users sampled completed specialized security training in FY 2009. These users were a VDC Service Manager, a Middleware Administrator, and a Senior Network Specialist, all with elevated privileges and responsibilities.

The VDC and the hosted systems contain or protect an enormous amount of confidential information (personal records, financial information, and other PII), and perform vital organization functions. Third parties might target the systems by exploitation, but the systems could also be targeted by trusted parties inside the contractor's organization. Without adequate operational and technical security controls in place, the Department's systems and information are vulnerable to attacks that could lead to a loss of confidentiality due to unauthorized access to data and to a possible loss of integrity through data modification or limited availability from unauthorized access and excessive use of system resources. Also, there is increased risk that unauthorized activities may occur that reduce the reliability of Department systems and data being maintained by the VDC and increases the potential that sensitive data may be released, used, or modified.

In response to our draft report, FSA thanked the OIG for the extensive effort in support of this audit and concurred or partially concurred with all of the findings identified except one. FSA did not concur with Finding Issue 4b about FSA's conflicting guidance. FSA stated that the report provides objective details it will use to improve FSA's comprehensive action plan to enhance information technology security. Additionally, FSA stated that all actions associated with the recommendations in this report will be entered into and tracked through the Department's audit resolution process as part of its Plans of Actions and Milestones process. We summarized and responded to specific comments in the "Findings" section of the audit report. We revised Recommendation 7.1 based on FSA's comments. FSA's response is included as an enclosure to this audit report.